

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT & ARREST WARRANT

I, Michael Peck, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service ("USSS") and have been so employed since 2006. I received formal training at the Federal Law Enforcement Training Center ("FLETC") in Glynco, Georgia, and the United States Secret Service Academy in Beltsville, Maryland. I am currently assigned to the United States Secret Service, Manchester Resident Office. My current assignment includes investigating federal offenses, including but not limited to those involving financial fraud and related activities.
2. As set forth below, the USSS is currently investigating Maine resident John Bryan Villegas ("target" or "suspect"), for engaging in a type of extortion known as "sextrortion." The target attempted to extort a New Hampshire resident (hereinafter "Victim") into providing sexually explicit photographs and videos of Victim by threatening to publish on the internet, and distribute to Victim's neighbors and work and social acquaintances, other sexually explicit photographs of Victim that were stored on her laptop computer which was stolen during a burglary of her residence.
3. The victim is a female who resides in Dover, New Hampshire, with her young child. Villegas is a social acquaintance of the Victim's; he is married to Victim's friend.
4. In summary, between July 10-July 16, 2012, the target, remaining anonymous and using the email address "████████@gmail.com," engaged in a series of e-mail exchanges with Victim. In those exchanges, the target advised Victim that the target has "a lot" of "x-rated" photographs of Victim in his possession. As proof, he then proceeded to describe, in detail, various sexually explicit photographs of her and sent her several sample photographs, including images of Victim fully nude and engaging in various sexual acts. The target then directed Victim to take new photographs and/or videos of herself engaging in various sexually explicit scenarios and to then send these new photographs and videos to him. Victim told the target that she was worried about her reputation and was afraid he would send the photos to others. The target responded that, if Victim did not provide him the "portfolio" or "show" he had requested, he would "dox" her, or, as he explained, would leak the photographs and other personal information about her on the internet. He also said that he knew where she resided, her less than ████████ son's name, her boyfriend's name, her ex-husband's name, and where she worked. He told her that if she did not provide him with the requested sexually explicit images, he would send the ones that he already had throughout Dover, New Hampshire, as well as to her ex-husband, boyfriend, and a recent former employer.
5. I am submitting this affidavit in support of a Criminal Complaint and Arrest Warrant, attached.

6 Based on my training and experience, and the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 875(d) and 1030(a)(7), each of which are felonies, have been committed by Villegas. The facts set forth in this affidavit are based upon my personal observations, my review of documents and computer records, my training and experience, and information obtained from other agents, including the primary case agent Matthew O'Neill, and witnesses, including from other law enforcement agents. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

II. PROBABLE CAUSE

7. Your affiant believes that there is probable cause to believe that violations of Title 18, United States Code, Sections 875(d) and 1030(a)(7)(B) have been committed by Villegas for the following reasons:

Title 18, United States Code, Section 875(d) states

§ 875. Interstate communications

...
(d) Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years, or both.

Title 18, United States Code, Section 1030(a)(7)(B) states:

§ 1030. Fraud and related activity in connection with computers

(a) Whoever—

...
(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any--

...
(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

shall be punished as provided in subsection (c) of this section.

LAPTOP BURGLARY AND E-MAIL EXCHANGE DEMANDING SEXUALLY EXPLICIT PHOTOS AND VIDEOS

8. On April 7, 2012, the Dover, NH, Police Department responded to a complaint about a burglary that occurred at a local residence. Victim lives with her young child who is [REDACTED] at the residence that was burgled. Victim told the Dover police detective that, during that burglary, multiple items were stolen, to include several pairs of Victim's underwear and her Apple MacBook Pro laptop computer (serial# [REDACTED]). During subsequent interviews Special Agent O'Neill had with the Victim, she reported that the stolen laptop contained private photographs of her that are of a sexual nature. The photographs were taken over the course of several years and by approximately three different people. To her knowledge, the photos had never been transferred to any other person, nor had they been published or uploaded onto any type of website. She reported that virtually all of the photographs were taken at her residence, with her own digital cameras (both of which remain in her possession), and the images were stored only on her cameras, the disk within her camera, and on her now stolen laptop computer.
9. On or about July 10, 2012, Victim began receiving multiple email messages that identified the sender (referred to herein as "target" or "suspect") with the email address: "[REDACTED]@gmail.com." The Victim reported that her maiden name is "[REDACTED]" but that she did not recognize the sender's e-mail address. A series of e-mail exchanges occurred between the Victim and the target, and with the Victim's permission, Special Agent O'Neill reviewed copies of those e-mail messages and excerpted relevant portions below. Those e-mails have travelled in interstate commerce.
10. On or about July 10, 2012, the target sent an email to Victim that stated, "what if I told you I have "pics" of you? Like a lot. Would you send me more?" Victim replied by email: "And who would this be?" On July 11, 2012, the target replied in an email, "a 'photographer' you look good modeling. Too bad for the lighting...you look good in a corsette too so send me more? You're crazy hot." Victim asked the target via email "And how have you seen these pictures of me?" The target answered, via email, "someone sent them to me. Show me more."
11. Also on July 11, 2012, Victim sent an email to [REDACTED]@gmail.com that states "Hmmmm I don't know who would give them to you. What kind of photographer are you?" The target, again through email account [REDACTED]@gmail.com, replied "there's also one of you on your knees in the shower , and a shot in the shower from behind. You really are crazy hot. I also love the pictures of you and your friend in sexy underwear with what looks like a bong."

12. Victim emailed the target and asked "Who sent you them again? I'm just confused how you would have seen something like that." The target replied via email, "it was like a random email, numbers and stuff, like the ones on craigslist. But they were pretty x-rated like you in lingerie being fucked from behind. Nudes of you, and some more stuff. It was a lot of pictures."
13. In a separate email on July 11, 2012, the target told Victim, "I don't mind getting rid of these. But can I see more of you at least." Victim replied, "Do you still have the email? Maybe I would recognize it or something." The target responded, "sure. Not for free though." Victim answered, "What are we talking about here?" The target answered, "I want to see more of you, well technically I have already seen all of you. I just wanna see more." Victim responded, "I don't even know who you are though." The target told Victim, "true. But same can also be said about you. I can just bugger off and keep all the pictures I received, and not give you a couple of the emails I received them from."
14. Continuing on July 11, 2012, the target, in another email, told Victim, "ok, go ahead and send me stuff, and the more you send me and the more you show me, the more I'll give you information." Victim replied to ask, "Did you have anything in mind?" The target then went on to describe various sexually explicit poses and other photos or videos he would like to see Victim provide. Victim answered, "and if I do that you'll tell me who emailed you?" The target told Victim, "Yes. I'll cooperate with you as much as I can. Here's your first piece of information...that person is using multiple emails because I received emails from different ones and they're still coming in. randomly. Now send me a LOT of stuff gorgeous. Drive me crazy."
15. Also on July 11, 2012, the target sent Victim an email that contained five attachments, four of which were images of Victim. Two of the attached images show Victim with her breasts fully exposed. Image #3 shows Victim laying on a bed wearing a t-shirt and underwear while eating dessert. Image #4 shows Victim wearing a bra and blue jeans while gesturing toward the camera. Image #5 is not recognizable. On the same date, the target, using the same email address, sent Victim an email that contained four attachments, three of which were images of Victim. The first attachment appears to be the same as image #5 from the aforementioned email. Images two through four show Victim wearing a tank top and looking at the camera. Victim reported that these photographs were among the private photographs located on her stolen laptop.
16. On the same date, the target emailed Victim to state, "bonus points for you beautiful if you use toys and actually get off on camera. Make it a long one baby tease me." Acting at the direction of the Dover police detective, Victim replied, "I'll see what I can do I'm not home right now. Anything else?" The target responded, "you can get loud for me ;) close ups as well gorgeous." The target also emailed Victim to add, "actually, wanna send me something to hold me over for now? ;) like sneak in to a ladies' room somewhere really quick and snap some hot sexy photos for me."
17. During email exchanges with Victim on July 12, 2012, the target stated that he is a photographer and that Victim should make a "portfolio" of sexually explicit photographs

for him. Acting at the direction of the Dover police detective, Victim told the target that she was interested in modeling but doesn't know any photographers near her. Specifically, Victim wrote, "Well you've obviously seen my pictures I'm not shy lol so I mean I'm interested if you are." The target tells Victim "Oh trust me I'm interested, but like I said, Hun, I'm pretty expensive ,) to be quite honest I'm based on the west coast so I barely know anyone around there, I can try and ask around? I mean I can still help you set up a portfolio if anything. Go to this one website called model mayhem and set up an account that should help you look for a photographer around you. Now doll, where's that video of mine? ;)"

18. On July 12, 2012, again acting at the direction of the Dover police detective, Victim emailed the target a photograph of her face and her stomach and wrote, "Hey so on a side note, I sent you a little something how about you tell me about that email?" The target replied, "hey now, that was one picture haha ;) I gotta get greedy, and besides I told you information first remember? ;) but hey here's one of the emails used I think it's literally a craigslist account [REDACTED]@job.craigslist.org . so how bout the rest of my 'payment.'"
19. On July 15, 2012, the target sent Victim an email that contained no text but contained five sexually explicit photos of Victim. These photos were among the private, undistributed photos contained on Victim's now stolen laptop.
20. On July 16, 2012, at the direction of the Secret Service, Victim sent the target an email telling him that she was concerned about her reputation and wanted to make sure that the photographs did not get sent to others. She wrote: "You know I thought more about it and I'm a little concerned about who else you may be sending these photos to. I still don't even understand how you have them to begin with and if they get out it'll ruin my reputation. I'm trying to start a new life and this would absolutely fuck everything up I'm trying to accomplish. I don't even know who the hell you are and why you actually have them." She also asked him what he would do if she refused to provide the sexually explicit "show" or photographs of herself that the target had demanded.
21. On that same date, the target replied in a series of e-mail messages: "alright [sic] be like that then. see what i do with these . . . think im [sic] a sick bastard? then im [sic] going to act like one. familiar with doxing? look it up. have fun! . . . i told you call me a sick bastard Im going to act like one . . . definition of DOXING leaking Personal information about people on the Internet, often including real name, known aliases, email addresses, general location, pictures . . ." In one email message, the target referenced a number of personal details about the victim, including the name of Victim's young child, with whom she resides, their physical address, the name of her current boyfriend, and the name of the restaurant where she worked until recently.
22. On July 16, 2012, at the direction of the Secret Service, Victim continued in an e-mail, "Listen I'm sorry I was nasty earlier I just don't want these photos getting out. I don't want my info being leaked or anything please I have a family and I can't risk my sons [sic] safety. Please don't", and the target replied, "yeah i agree. so i bet now you're [sic]

more willing to comply to my request? see we do have a thing going. If you're still willing to do your portfolio. Im [sic] still here to help."

23. Also on July 16, 2012, the target again threatened to distribute the photographs to others, including Victim's former employer, former husband, and boyfriend. He wrote, "Do you think [name of Victim's former employer] would be able to appreciate these artistic shots? Uhm [first and last name of Victim's ex-husband]? Or [first name of Victim's boyfriend]? Would they be able to appreciate these? Im [sic] really looking forward to your reply." He followed up withm "That's fine just ignore me I'll send envelopes of pictures to places around Dover, NH and [the Victim's former employer]."

TARGET'S IDENTITY AS JOHN BRYAN VILLEGENAS

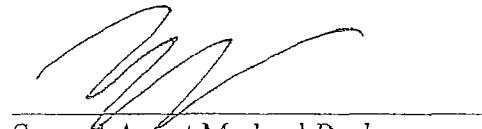
24. On July 16, 2012, Google advised that the e-mail account, [REDACTED]@gmail.com, was created on July 2, 2012, from IP address 214.1.3.248, and that a user logged in to this e-mail account from IP address 214.1.3.248 regularly between July 2, 2012 and July 16, 2012. That IP address resolves to the U.S. Navy and the Domain Name Server (DNS) records identify the IP address being named "nchne-wsa-dp.med.navy.mil." (Emphasis added). Additionally, a user logged in to this account from IP address 76.118.87.231 numerous times between July 11, 2012 and July 16, 2012. Open source subscriber information revealed that IP address 76.118.87.231 resolves to internet service provider, Comcast Cable. A user established a secondary account on or about July 12, 2012. The name for this account was [REDACTED] and email address [REDACTED]@gmail.com. Victim's former boyfriend currently lives with an individual named [REDACTED].

25. On July 16, 2012, Comcast Cable advised that IP address 76.118.87.231 is assigned to "Viligias," [REDACTED], Kittery, ME, telephone 207-[REDACTED].

26. Victim identified [REDACTED] Villegas (misspelled "Viligias" in the Comcast records) as her friend. [REDACTED] Victim stated that Villegas's husband, Bryan, works for the U.S. Navy.

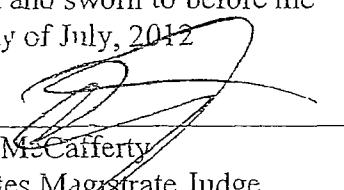
27. Law enforcement records confirm that "John Bryan Villegas" resides with "Villegas" at [REDACTED] Kittery, ME. Navy personnel have confirmed that John Bryan Villegas is [REDACTED] in the U.S. Navy [REDACTED] and works in a medical unit.

28. Based on my training and experience, and the facts as set forth in this affidavit, I submit that there is probable cause to believe that Villegas has violated 18 U.S.C. §§ 875(d), 1030(a)(7).



Special Agent Michael Peck
United States Secret Service

Subscribed and sworn to before me
this 17th day of July, 2012



Landya B. McCafferty
United States Magistrate Judge